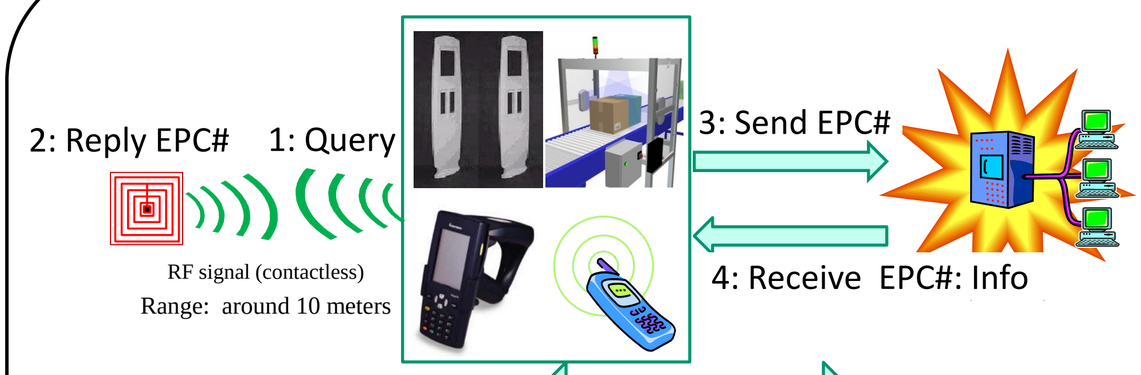
RFID Security and Privacy

SMU SINGAPORE MANAGEMENT UNIVERSITY

School of Information Systems

Associate Professor Yingjiu Li

WORKING IN RFID TECHNOLOGY



Tags

Attached to objects, give out their (unique) EPC# via RF signal

(EPC: Electronic Product Code)

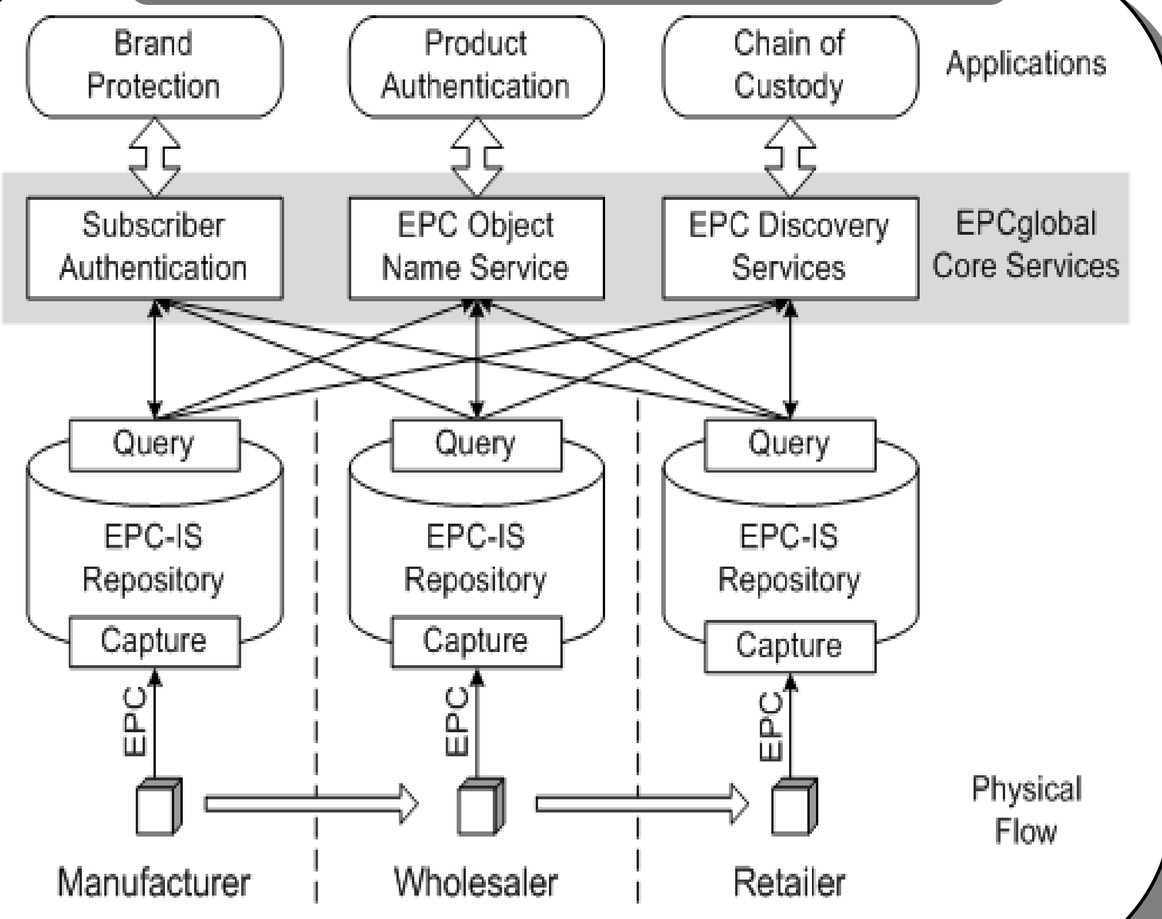
Readers

1. Query & read EPC# from tags via RF signal
2. Get more info. about EPC# from EPC-IS
3. Update EPC-IS: e.g., EPC# arrived at 10:53pm at location X

EPC-Information Services (EPC-IS)

Detailed real-time info about EPC# is constantly updated and maintained in here

WORKING IN EPC-GLOBAL NETWORK



CENTRAL CONCERNS & QUESTIONS

Adopting RFID technology is an emerging trend in industry as it enables product information to be collected, shared, and managed in real time. However, the RFID technology has also triggered significant security and privacy concerns as industry espionage may eavesdrop on wireless RFID communications and launch active attacks.

EMERGING IDEAS & INITIATIVES

The security and privacy concern in RFID systems should be addressed systematically, starting from formalization of security and privacy requirements, to the design, analysis, and evaluation of practical RFID systems according to the requirements.

FUNDING AND PEOPLE

• FUNDING: A Security Framework for EPCglobal Network. Public Sector Funding (PSF), A*STAR SERC, Aug 2009-Jan 2012.

• FUNDING: The Use of Mobile Devices in RFID-Based Supply Chain Management. Nokia Beijing, September 2009- September 2010.

•FACULTY / RESEARCH STUDENTS / RESEARCH STAFF: Yingjiu Li, Robert Deng, Xuhua Ding, Changshe Ma, Shaoying Cai, Qiang Yan, Bing Liang, Kuo-Hui Yeh, Junzuo Lai, Kevin Chiew, Chunhua Su, Ge Fu

• EXTERNAL COLLABORATORS: Tieyan Li, Yunlei Zhao, Ivy Zheng, Nai-Wei Lo, Wei He, Eng Wah Lee, Guilin Wang

RESEARCH HIGHLIGHTS

- Our major contribution in this field is to clarify the differences between two RFID privacy notions: one based on the indistinguishability of two tags (denoted as ind-privacy), and the other based on the unpredictability of the output of a protocol (denoted as unp-privacy). It is proven that ind-privacy is weaker than unp-privacy. Moreover, the minimal (necessary and sufficient) condition on RFID tags to achieve unp-privacy is determined.
- A new framework on RFID privacy is developed based on zero knowledge (i.e., the indistinguishability between a real tag and a simulated tag). This concept is stronger than ind-privacy, and more reasonable than unp-privacy in practice.
- A series of RFID protocols, including key distribution, reader-tag authentication, tag collision resolution, grouping proof, tag ownership transfer, and tag path authentication, are designed, analyzed, and evaluated to meet the secure and practical requirements in RFID applications such as RFID-enabled supply chains.

SELECTED PUBLICATIONS

1. Yingjiu Li, Robert Deng, Junzuo Lai, Changshe Ma: On Two RFID Privacy Notions and Their Relations. Accepted by ACM Transactions on Information and System Security (TISSEC), 2012.
2. Tieyan Li, Yingjiu Li, Guilin Wang: Secure and Practical Key Distribution for RFID-Enabled Supply Chains. 7th International ICST Conference on Security and Privacy in Communication Networks (SecureComm), London, UK, September 7-9, 2011.
3. Robert Deng, Yingjiu Li, Moti Yung, Yunlei Zhao: A New Framework for RFID Privacy. 15th European Symposium on Research in Computer Security (ESORICS), pages 1-18, Athens, Greece, September 20-22, 2010.
4. Changshe Ma, Yingjiu Li, Robert Deng, Tieyan Li: RFID Privacy: Relation Between Two Notions, Minimal Condition, and Efficient Construction. 16th ACM Conference on Computer and Communications Security (CCS 2009), pages 54-65, Chicago, US, November 9-13, 2009.